

# **PROPOSAL TUGAS AKHIR**



## **Rancang Bangun Sistem *E-Control* Tugas Akhir pada Jurusan Kriptografi Politeknik Siber dan Sandi Negara**

**Muhammad Irfan Cahyanto  
1817101438**

**Rekayasa Kriptografi  
Politeknik Siber dan Sandi Negara  
2021/2022**

# **PROPOSAL TUGAS AKHIR**



## **Rancang Bangun Sistem *E-Control* Tugas Akhir pada Jurusan Kriptografi Politeknik Siber dan Sandi Negara**

**Muhammad Irfan Cahyanto  
1817101438**

**Rekayasa Kriptografi  
Politeknik Siber dan Sandi Negara  
2021/2022**

## **LEMBAR PERSETUJUAN**

Proposal Tugas Akhir dengan:

JUDUL : Rancang Bangun Sistem *E-Control* Tugas Akhir pada Jurusan  
Kriptografi Politeknik Siber dan Sandi Negara

PENULIS : Muhammad Irfan Cahyanto

NPM : 1817101438

dinyatakan diterima dan disetujui untuk dipertahankan dalam Seminar Proposal  
Tugas Akhir Politeknik Siber dan Sandi Negara Angkatan 2018 tahun 2022

Bogor, 23 Desember 2021

Pembimbing Materi

Ray Novita Yasa, M.Si  
NIP 19921111 201902 2 001

## LEMBAR PENGESAHAN

Proposal Tugas Akhir dengan:

JUDUL : Rancang Bangun Sistem *E-Control* Tugas Akhir pada Jurusan  
Kriptografi Politeknik Siber dan Sandi Negara

PENULIS : Muhammad Irfan Cahyanto

NPM : 1817101438

diperiksa dan disahkan oleh Tim Penguji Seminar Proposal/Sidang Tugas Akhir di  
Bogor, pada tanggal 4 Januari 2022

Ketua Penguji

Penguji I

Raden Budiarto Hadiprakoso, MMSI  
NIP 19861017 201712 1 001

Ray Novita Yasa, M.Si  
NIP 19921111 201902 2 001

Penguji II

Hermawan Setiawan, S.Si., M.T.I.  
NIP 19740623 199312 1 1001

## DAFTAR ISI

	Halaman
LEMBAR JUDUL .....	i
LEMBAR PERSETUJUAN.....	ii
LEMBAR PENGESAHAN .....	iii
DAFTAR ISI.....	iv
DAFTAR TABEL.....	vi
DAFTAR GAMBAR .....	vii
BAB I PENDAHULUAN.....	1
I.1    LATAR BELAKANG.....	1
I.2    RUMUSAN MASALAH .....	4
I.3    PEMBATASAN MASALAH .....	4
I.4    TUJUAN DAN MANFAAT .....	4
I.4.1    Tujuan Penelitian .....	4
I.4.2    Manfaat Penelitian .....	5
BAB II TELAAH KEPUSTAKAAN .....	6
II.1    LANDASAN TEORI .....	6
II.1.1    Sistem <i>E-Control</i> Tugas Akhir.....	6
II.1.2    Jurusan Kriptografi Politeknik Siber dan Sandi Negara (Poltek SSN)	7
II.1.3 <i>Multi-factor Authentication</i> (MFA) .....	9
II.1.4    Serangan Injeksi SQL ( <i>Structured Query Language</i> ).....	10
II.1.5    Algoritma Blowfish.....	12
II.1.6 <i>Hypertext Preprocessor</i> (PHP) dengan <i>Framework</i> Codeigniter (CI)	12
II.1.7    OWASP Secure Coding Practices Quick Reference Guide .....	13
II.1.8 <i>System Prototyping</i> .....	14
II.2    PENELITIAN TERKAIT.....	16
II.2.1 <i>Online Thesis Guidance Management Information System</i> [4] .....	16
II.2.2    Sistem Aplikasi Pengelolaan Tugas Akhir Berbasis <i>Mobile</i> [3].....	16

II.2.3	<i>An Improved OTP Grid Authentication Scheme Email-based using Middle-square for Disaster Management System</i> [18] .....	17
II.2.4	Perbandingan Algoritma AES dan Blowfish untuk Pengamanan Data dalam <i>Database</i> pada Rancang Bangun Aplikasi Pengelolaan Surat berbasis Web Dinas Pendidikan Kota Mataram [11] .....	17
II.3	KERANGKA/MODEL KONSEPTUAL .....	19
BAB III METODOLOGI PENELITIAN.....		20
III.1	OBJEK PENELITIAN.....	20
III.2	JENIS PENELITIAN.....	20
III.3	DESAIN PENELITIAN .....	20
III.3.1	Research Clarification (RC).....	21
III.3.2	Descriptive Study I (DS I).....	22
III.3.3	Prescriptive Study (PS) .....	23
III.3.4	Descriptive Study II (DS II).....	28
III.4	JADWAL PENELITIAN.....	30
DAFTAR PUSTAKA .....		31
LAMPIRAN.....		33

## DAFTAR TABEL

	Halaman
Tabel II.1 <i>Field</i> Data pada Sistem <i>E-Control</i> Tugas Akhir .....	9
Tabel II.2 Perbandingan Penelitian Terkait .....	18
Tabel II.3 Kerangka Konseptual .....	19
Tabel III.1 Tahapan Perancangan dan Pengembangan Aplikasi.....	23
Tabel III.2 Atribut Diagram UML .....	25
Tabel III.3 Jadwal Penelitian.....	30

## DAFTAR GAMBAR

	Halaman
Gambar II.1 Alur Saat Pengajuan ICP .....	7
Gambar II.2 Alur Saat Pengajuan Proposal .....	8
Gambar II.3 Alur Saat Pengerjaan Tugas Akhir .....	8
Gambar II.4 Proses <i>Multi-factor Authentication</i> .....	10
Gambar II.5 Serangan Injeksi SQL [21] .....	11
Gambar II.6 Tahapan <i>System Prototyping</i> .....	15
Gambar II.7 Alur bisnis penelitian [4] .....	16
Gambar III.1 Skema <i>Design Research Methodology</i> .....	21
Gambar III.2 Skema Studi Literatur .....	21
Gambar III.3 Model Referensi .....	23



## **BAB I PENDAHULUAN**

### **I.1 LATAR BELAKANG**

Adanya virus COVID-19 sejak Maret 2020 membuat pemerintah Indonesia menetapkan kebijakan untuk menerapkan metode Pendidikan Jarak Jauh untuk pendidikan tinggi [1] yang menyebabkan komunikasi secara langsung antara mahasiswa dan dosen masih sangat terbatas [2]. Tugas akhir menjadi salah satu kegiatan yang membutuhkan tingkat komunikasi mahasiswa dan dosen yang cukup intens sebab mahasiswa selalu dibantu dan dikontrol oleh dosen pembimbing dalam proses pengerjaannya. Tugas akhir disusun oleh mahasiswa tingkat akhir sebagai syarat untuk menyelesaikan studi pada pendidikan tinggi [3].

Pengelolaan dan kontrol tugas akhir yang baik pada sebuah instansi pendidikan tentu akan mempermudah para pihak yang terlibat dalam proses pelaksanaannya [3]. Penelitian Simatupang dan Muhammad [3] di Amik Mahaputra Riau (AMP) menyatakan pengelolaan tugas akhir pada perguruan tinggi secara umum masih dilakukan dengan cara manual (kertas) mulai dari pengajuan judul, pelaksanaan bimbingan sampai dengan pengolahan data hasil tugas akhir sehingga menimbulkan beberapa masalah. Untuk itu dibutuhkan sebuah sistem atau aplikasi untuk menyelesaikan hal tersebut. Akhirnya, hasil aplikasi pengelolaan tugas akhir tersebut membantu mahasiswa kapan dan dimana saja dapat mengakses dan melihat informasi terkait tugas akhir tanpa batas waktu dan jarak. Kemudian, penelitian Nasution *et al* [4] menyatakan perkembangan teknologi internet dalam dunia pendidikan masih belum maksimal, terutama dalam proses bimbingan tugas akhir antara mahasiswa dengan dosen. Kesulitan yang ditemui dosen untuk membantu mahasiswa selama bimbingan skripsi adalah keterbatasan waktu komunikasi dan kesesuaian jadwal antara mahasiswa dengan dosen. Untuk mengatasi masalah tersebut, dirancang sistem informasi manajemen bimbingan tugas akhir yang membantu mahasiswa dan dosen untuk melakukan proses bimbingan kapan saja dan di mana saja.

Politeknik Siber dan Sandi Negara (Poltek SSN) merupakan salah satu instansi pendidikan yang meluluskan mahasiswa setiap tahunnya dengan syarat menyelesaikan tugas akhir. Menurut Bapak Dion Ogi selaku Ketua Jurusan Kriptografi Poltek SSN, pengelolaan tugas akhir di Jurusan masih menggunakan administrasi manual yakni dengan mengirimkan tautan pendaftaran maupun pengumpulan tugas akhir kepada mahasiswa dan dosen secara langsung. Hal ini mengakibatkan lamanya waktu dan sering terjadi keterlambatan dalam pengumpulan laporan perkembangan. Kemudian juga proses kontrol bimbingan yang tidak bisa dipantau oleh jurusan secara langsung, ada juga ketidaklengkapan

dan ketidaksesuaian *file* yang seharusnya dikumpulkan oleh mahasiswa. Alangkah baiknya jika terdapat suatu sistem yang memfasilitasi permasalahan-permasalahan tersebut. Untuk itu, penelitian ini akan merancang dan membangun sistem *e-control* tugas akhir berbasis web untuk mahasiswa dan dosen dalam mempermudah proses kontrol jurusan dan dosen khususnya pembimbing terhadap mahasiswa terkait. Adapun alur pengerjaan tugas akhir di Politeknik Siber dan Sandi Negara diawali dengan pengajuan *Idea Concept Project* (ICP) oleh mahasiswa kepada jurusan, setelah menerima persetujuan kemudian menentukan dosen pembimbing untuk melakukan pengerjaan proposal untuk diseminarkan. Setelah nantinya proposal tugas akhir sudah disetujui oleh dosen pembimbing dan penguji, dilanjutkan pada tahap pengerjaan tugas akhir. Adapun prosesnya yakni penyelesaian tugas akhir 30%, 70% kemudian seminar, lalu 100% dan ditutup dengan sidang tugas akhir. Setelah dinyatakan lulus pada sidang tugas akhir, mahasiswa dapat dinyatakan lulus pendidikan pada instansi pendidikan Politeknik Siber dan Sandi Negara.

Salah satu elemen dalam tugas akhir yaitu data. Berdasarkan Keputusan Ketua Sekolah Tinggi Sandi Negara Nomor 1 Tahun 2011 tentang Pedoman Tugas Akhir, data atau informasi merupakan salah satu aspek yang harus dijaga kerahasiannya [5] terlebih data pribadi dan data tugas akhir karena termasuk karya ilmiah. Hal ini juga didukung oleh UU No 24 Tahun 2014 tentang Hak Cipta. Pasal 1 ayat 3 menyebutkan bahwa yang disebut ciptaan adalah setiap hasil karya cipta di bidang ilmu pengetahuan, seni dan sastra yang dihasilkan atas inspirasi, kemampuan, pikiran, imajinasi, kecekatan, keterampilan, atau keahlian yang diekspresikan dalam bentuk nyata. Kemudian pasal 40 ayat 1 menyebutkan ciptaan yang dilindungi meliputi ciptaan dalam bidang ilmu pengetahuan, seni, dan sastra, dan salah satunya adalah semua hasil karya tulis lainnya termasuk tugas akhir [6].

Namun, menurut Patroli Siber [7] pencurian dan kebocoran data justru semakin meningkat dari tahun ke tahun. Tercatat sebanyak 182 kasus pencurian data dilaporkan oleh masyarakat pada 2020. Angka ini meningkat 27,3% dibandingkan dengan tahun sebelumnya yang sebanyak 143 laporan. Selama lima tahun terakhir, peningkatan laporan pencurian data meningkat 810% dari awalnya 20 laporan pada 2016. Bahkan sertifikat vaksinasi presiden beredar di sosial media. Selain data presiden, kasus kebocoran juga pernah terjadi pada Mei 2021. Kurang lebih 279 juta data peserta BPJS Kesehatan diperjualbelikan di RaidForums [7]. Kejadian tersebut dapat merugikan masyarakat luas bahkan negara.

Adanya pencurian dari kebocoran data dapat disebabkan oleh sistem yang diserang dengan injeksi SQL pada *database*. Saat ini, serangan injeksi SQL (*Structured Query Language*) masih masuk dalam daftar 10 besar OWASP (*Open Web Application Security Project*) tahun 2021 [8] yang artinya kerawanan pada web akibat serangan ini masih tinggi bahkan tahun 2017 menduduki posisi pertama.

Pada tahun 2021 sebanyak 94% aplikasi diuji dalam beberapa bentuk injeksi dengan tingkat kejadian maksimum 19% dan tingkat kejadian rata-rata 3,37% [8]. Dengan data tersebut, perlu adanya sebuah metode agar informasi dalam *database* aman dari pihak yang tidak berwenang. Salah satu caranya yakni dengan menggunakan algoritma kriptografi. Menurut Singh [9] mengenai perbandingan algoritma enkripsi menggunakan kunci simetrik dan asimetrik bahwa algoritma enkripsi menggunakan kunci simetrik lebih baik dalam hal kecepatan dan konsumsi daya. Beberapa algoritma enkripsi kunci simetrik menurut Meko [10] yaitu DES, AES, IDEA, dan Blowfish yang memiliki kelebihan dan kekurangan masing-masing dalam proses enkripsi dan dekripsi data yang dilihat dari segi kecepatan maupun keamanan data *ciphertext* yang dihasilkan. Penelitian Diancaraka [11] menyebutkan dari perbandingan algoritma Blowfish dan AES didapatkan hasil enkripsi dan dekripsi Blowfish membutuhkan waktu lebih kecil daripada AES serta *maximum throughput* yang dihasilkan Blowfish lebih tinggi dibandingkan AES. Ini berarti algoritma Blowfish lebih cocok digunakan untuk pengamanan data. Penggunaan algoritma enkripsi ini bertujuan untuk melakukan pengamanan data yang disimpan pada *database* sebagai bentuk pengamanan dari serangan injeksi SQL. Pada penelitian ini juga akan diterapkan *secure coding* untuk menambah pengamanan sistem terhadap serangan injeksi SQL.

Sistem *e-control* tugas akhir juga akan dibangun dengan menerapkan *multi-factor authentication* (MFA). MFA adalah salah satu kontrol paling efektif yang dapat diterapkan sistem untuk mencegah musuh mendapatkan akses ke perangkat atau jaringan dan mengakses informasi sensitif [12]. Penerapan MFA dikarenakan pada era digital saat ini autentikasi faktor tunggal seperti *password*, tidak lagi dianggap aman [13]. MFA pada penelitian ini menggunakan *password* dan kode *one time password* (OTP) pada *email*. OTP dapat digunakan untuk menambah lapisan keamanan autentikasi [14].

Pada penelitian ini akan merancang dan membangun sistem *e-control* tugas akhir berbasis web yang kemudian menerapkan MFA untuk akses ke sistem (*login*) dan *secure coding* berdasarkan OWASP *Secure Coding Practices Quick Reference Guide* guna pengamanan data pada sistem dari serangan injeksi SQL. Pengembangan sistem akan menggunakan *Design Research Methodology* (DRM) dengan menggunakan metode pengembangan model *prototyping*. Penggunaan model *prototyping* karena berfokus pada pengembangan sistem untuk memenuhi persyaratan pihak terkait sehingga dapat memperbaiki kembali sistem yang dibangun [9]. Kemudian sistem yang dibangun diharapkan dapat memenuhi kebutuhan Jurusan Kriptografi Poltek SSN sebagai bentuk kontrol secara langsung terhadap mahasiswa dan dosen pembimbing dalam proses penyelesaian tugas akhir.

## I.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan, rumusan permasalahan dalam penelitian Tugas Akhir ini, yaitu:

- a) Apakah sistem *e-control* tugas akhir dapat memenuhi kondisi yang diharapkan oleh Jurusan Kriptografi Politeknik Siber dan Sandi Negara?
- b) Apakah penerapan *multi-factor authentication* (MFA) dan *secure coding* dapat mengamankan proses autentikasi dan mengamankan data dari serangan injeksi SQL pada sistem *e-control* tugas akhir?

## I.3 PEMBATASAN MASALAH

Dalam penelitian ini, terdapat beberapa pembatasan yang digunakan, yaitu :

- a) Lokus penelitian hanya pada Jurusan Kriptografi Poltek SSN.
- b) Sistem *e-control* tugas akhir dibangun berbasis web dengan *database* MySQL.
- c) *Multi-factor authentication* (MFA) yang dimaksud adalah *password* dan *one time password* (OTP) pada email.
- d) Bahasa pemrograman yang digunakan adalah PHP dengan framework Code Igniter.
- e) Jenis *file* yang digunakan pada sistem berupa dokumen dengan ekstensi PDF.
- f) Pada penerapan *secure coding* hanya menggunakan lima daftar periksa yaitu *Input Validation*, *Authentication and Password Management*, *Data Protection*, *Database Security*, dan *File Management*.
- g) Tahap pengujian dilakukan pada server lokal (*localhost*).
- h) Serangan dilakukan untuk menyerang *database* menggunakan injeksi SQL.
- i) Tidak membahas mengenai serangan pada algoritma Blowfish.

## I.4 TUJUAN DAN MANFAAT

Berikut merupakan tujuan dari penelitian ini serta manfaat yang dapat diambil.

### I.4.1 Tujuan Penelitian

Tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut:

- a) Merancang dan membangun sistem *e-control* tugas akhir berbasis web untuk mahasiswa dan dosen di Jurusan Kriptografi Poltek SSN.
- b) Untuk mengetahui hasil penerapan *multi-factor authentication* (MFA) dan *secure coding* pada sistem dalam mengamankan proses autentikasi dan data yang ada.

#### **I.4.2 Manfaat Penelitian**

Dalam penelitian ini, terdapat beberapa manfaat yang diperoleh, yaitu:

- a) Membantu Jurusan Kriptografi Poltek SSN dalam mendukung program PJJ pemerintah.
- b) Pilihan alternatif kontrol bimbingan dalam mengurangi pertemuan tatap muka secara langsung antara mahasiswa dan dosen karena sedang di masa pandemi.
- c) Sebagai sarana pembelajaran bagi penulis dalam membangun aplikasi berbasis web dengan melakukan pengamanan autentikasi dan *database*.

## BAB II TELAAH KEPUSTAKAAN

### II.1 LANDASAN TEORI

#### II.1.1 Sistem *E-Control* Tugas Akhir

Pada tahun 2015, penelitian Nuryana dan Mulyani [15] menyatakan 98% mahasiswa Sekolah Tinggi Teknologi Garut yang mengambil mata kuliah skripsi membutuhkan aplikasi kontrol skripsi untuk membantu proses skripsi. Hasilnya aplikasi pengendalian skripsi dapat membantu mahasiswa dan dosen dalam proses pelaksanaan mata kuliah skripsi seperti pelaporan *progress* laporan bimbingan, pencarian informasi seputar skripsi dan lainnya.

Pada tahun 2017, penelitian Nasution *et al* [4] menyatakan perkembangan teknologi internet dalam dunia pendidikan masih belum maksimal, terutama dalam proses bimbingan tugas akhir antara mahasiswa dengan dosen. Kesulitan yang ditemui dosen untuk membantu mahasiswa selama bimbingan skripsi adalah keterbatasan waktu komunikasi dan kesesuaian jadwal antara mahasiswa dengan dosen. Untuk mengatasi masalah tersebut, dirancang sistem informasi manajemen bimbingan tugas akhir yang membantu mahasiswa dan dosen untuk melakukan proses bimbingan kapan saja dan di mana saja. Hasilnya aplikasi bimbingan tugas akhir ini dapat membantu proses komunikasi antara mahasiswa dengan dosen dan mempermudahnya.

Pada tahun 2019, penelitian Simatupang dan Muhammad [3] di Amik Mahaputra Riau (AMP) menyatakan pengelolaan tugas akhir pada perguruan tinggi secara umum masih dilakukan dengan cara manual (kertas) mulai dari pengajuan judul, pelaksanaan bimbingan sampai dengan pengolahan data hasil tugas akhir sehingga menimbulkan beberapa masalah. Diantaranya pengajuan judul, mahasiswa harus mengisi formulir pengajuan judul kemudian diserahkan ke program studi, terkadang formulir tersebut hanya diarsipkan saja sehingga formulir tersebut tercecer bahkan hilang. Oleh karena itu tidak jarang mahasiswa harus mengisi kembali formulir pengajuan judul. Pendataan mahasiswa yang telah mengajukan judul, pada proses pendataan ini anggota program studi harus memeriksa dan mencatat satu persatu formulir yang diajukan oleh mahasiswa sehingga pendataannya membutuhkan waktu yang relatif lama dan terkesan sangat lambat. Kemudian untuk pengumuman hasil pengajuan judul, anggota program studi harus memeriksa dan mencatat satu persatu berita acara hasil seminar proposal, kemudian membuat rekap seminar hasil sehingga prosesnya juga membutuhkan waktu yang relatif lama. Untuk itu dibutuhkan sebuah sistem atau aplikasi untuk menyelesaikan hal tersebut. Akhirnya, hasil aplikasi pengelolaan tugas akhir tersebut membantu

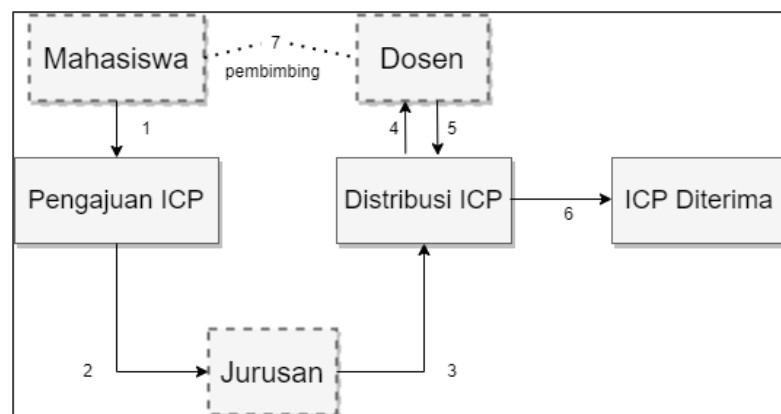
mahasiswa kapan dan dimana saja dapat mengakses dan melihat informasi terkait tugas akhir tanpa batas waktu dan jarak.

Dari penelitian-penelitian tersebut, sistem atau aplikasi *e-control* tugas akhir dibutuhkan oleh perguruan tinggi guna membantu dalam proses penyelesaian tugas akhir mahasiswa. Kemudian penelitian ini akan merancang dan membangun sistem yang disebut *e-control* tugas akhir berbasis web dengan fitur dan aktornya menyesuaikan lokus penelitian yaitu pada Jurusan Kriptografi Politeknik Siber dan Sandi Negara.

### II.1.2 Jurusan Kriptografi Politeknik Siber dan Sandi Negara (Poltek SSN)

Peraturan Badan Siber dan Sandi Negara Nomor 12 Tahun 2019 tentang Organisasi dan Tata Kerja Politeknik Siber Dan Sandi Negara, pasal 22 menyebutkan bahwa jurusan merupakan salah satu unsur pelaksana pendidikan [16]. Ini berarti Jurusan Kriptografi merupakan salah satu pelaksana pendidikan di Politeknik Siber dan Sandi Negara (Poltek SSN) yang dahulu disebut Sekolah Tinggi Sandi Negara (STSN). Mahasiswa tingkat akhir wajib menyelesaikan tugas akhir sebagai syarat kelulusan pendidikan untuk memperoleh gelar Diploma IV (D4). Berdasarkan Keputusan Ketua Sekolah Tinggi Sandi Negara Nomor 1 Tahun 2011 tentang Pedoman Tugas Akhir, tugas akhir (TA) adalah karya ilmiah yang disusun menurut kaidah keilmuan dan ditulis berdasarkan Bahasa Indonesia yang baku, di bawah pengawasan atau pengarahan dosen pembimbing, untuk memenuhi kriteria-kriteria kualitas yang telah ditetapkan [5].

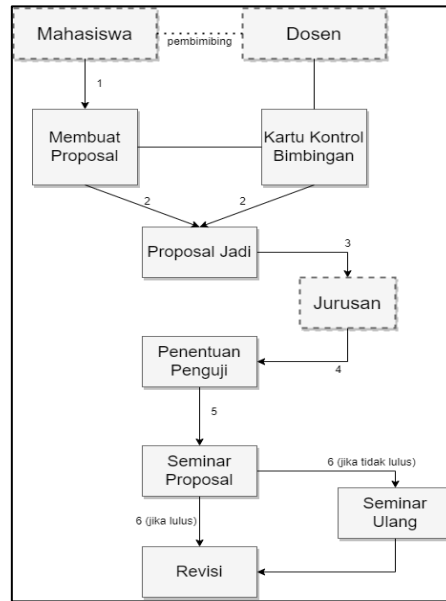
Jurusan memiliki kewajiban untuk mendukung proses penyelesaian tugas akhir mahasiswa Poltek SSN. Salah satu caranya yakni dengan memberikan layanan administrasi terhadap mahasiswa dan dosen dalam proses penyelesaian tugas akhir, mulai dari pengajuan *Idea Concept Project* (ICP), proposal, seminar, dan tugas akhir itu sendiri. Terdapat tiga proses bisnis yang dibagi atas waktu pengerjaan tugas akhir. Berikut alur bisnis untuk ICP pada Gambar II.1.



Gambar II.1 Alur Saat Pengajuan ICP

Sumber: diolah kembali dari hasil wawancara Lampiran 1

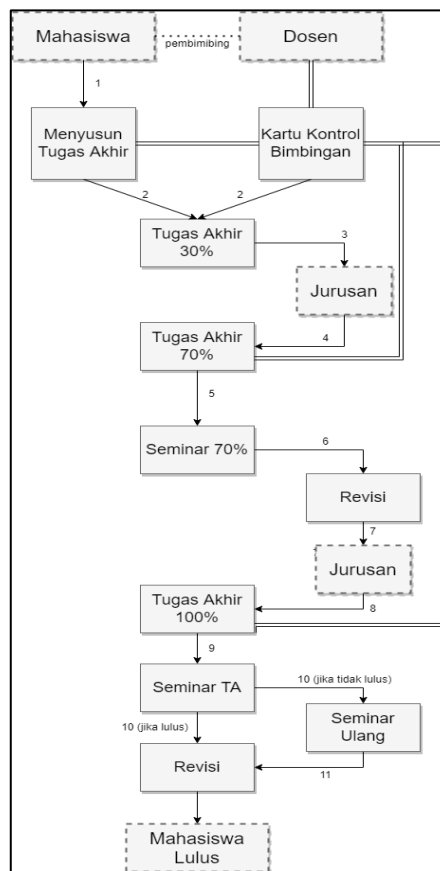
Kemudian berikut Gambar II.2 adalah alur bisnis untuk proposal dan seminarnya.



Gambar II.2 Alur Saat Pengajuan Proposal

Sumber: diolah kembali dari hasil wawancara Lampiran 1

Selanjutnya berikut Gambar II.3 adalah alur bisnis untuk penyusunan tugas akhir.



Gambar II.3 Alur Saat Pengerjaan Tugas Akhir

Sumber: diolah kembali dari hasil wawancara Lampiran 1



Adapun *database* yang digunakan pada sistem disesuaikan dengan kebutuhan lokus yakni Jurusan Kriptografi Poltek SSN. Adapun aktor-aktor yang terlibat nantinya adalah admin, mahasiswa, dosen, dan dosen yang merangkap sebagai Ketua Jurusan dan Ketua Prodi. Berikut merupakan tabel *field* datanya yang disimpan dalam *database* MySQL:

Tabel II.1 *Field* Data pada Sistem *E-Control* Tugas Akhir

Sumber: diolah dari hasil lampiran 1

TugasAkhir	IDTa, IDMahasiswa, JudulTa, FileProposal, FileTa, TanggalUpload
Prodi	IDProdi, NamaProdi
User	ID, Nama, Password, IDProdi, Email, Foto Status
Admin	IDAdmin, Username, Password
KartuBimbingan	IDKartu, IDKartuMahasiswa, IDKartuDosen, Catatan, TanggalBimbingan

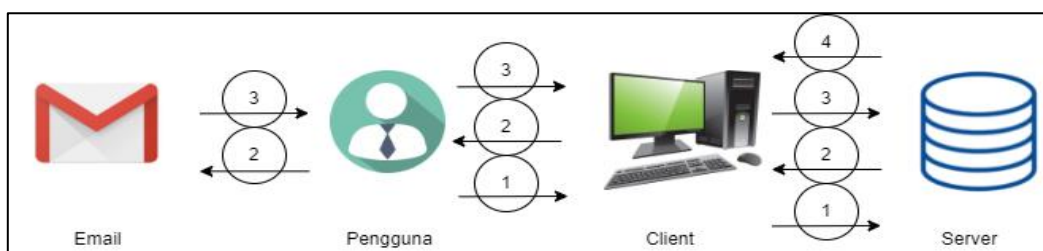
### II.1.3 *Multi-factor Authentication* (MFA)

Sistem perangkat lunak memiliki banyak metode dalam pengamanannya. Salah satu faktor dasar yang digunakan untuk pengamanan sistem yakni menerapkan proses autentikasi data pengguna. Autentikasi adalah penggunaan salah satu atau lebih banyak mekanisme untuk mengonfirmasi bahwa entitas yang meminta akses adalah entitas yang sah. Setelah identitas sah atau mesin memvalidasi, akses ke sistem akan diberikan [13].

Autentikasi yang diterapkan dapat dilakukan dengan berbagai metode, salah satunya adalah *password*. Perkembangan era digital yang pesat menjadikan autentikasi faktor tunggal, seperti *password* tidak lagi dianggap aman. Permasalahannya adalah perilaku pengguna cenderung menggunakan *password* yang entropi dan lemah [17]. Ketidakamanan pengguna dalam berperilaku menjadikan kebutuhan autentikasi yang dapat meningkatkan keamanan sistem.

Kelemahan autentikasi faktor tunggal dapat diatasi dengan *multi-factor authentication* (MFA). MFA yakni kerangka kerja keamanan lebih dari satu *password* konfirmasi dijalankan untuk memastikan keaslian entitas [13]. Penggunaan MFA dapat memperkuat sistem terutama jika diterapkan pada proses *login*. MFA akan meningkatkan keamanan informasi dan meningkatkan keamanan sistem web [17].

Penelitian ini akan membangun sistem *e-control* berbasis web dengan menerapkan MFA menggunakan password dan kode *one time password* (OTP) yang akan dikirimkan ke email. OTP adalah *string* karakter dan atau angka yang digunakan untuk autentikasi yang hanya berlaku untuk satu transaksi atau sesi sebanyak 4-6 karakter dan atau angka. Kode ini juga memiliki keterbatasan waktu untuk mengaksesnya sehingga jika melewati waktu tersebut, kode akan tidak berlaku lagi dan akan digantikan dengan kode yang baru. OTP dapat meningkatkan keamanan pengguna karena akan mencegah dari *brute force attack*, *dictionary attack*, *insider attack*, dan *key-logger attack* [18]. Proses MFA berdasarkan [19] menyesuaikan atribut pada sistem sebagai berikut:



Gambar II.4 Proses *Multi-factor Authentication*

1. Pengguna masuk situs web *e-control* dan meminta akses *login*. Kemudian permintaan dikirim ke server, kemudian server meminta pengguna memasukkan *username* dan *password*. Jika *username* dan *password* benar, maka sistem akan meminta input kode OTP.
2. Server mengirimkan kode acak OTP ke email pengguna.
3. Pengguna menginputkan kode OTP dan server memvalidasi kode OTP.
4. Jika kode yang dimasukkan benar, pengguna dapat mengakses sistem. Jika salah, permintaan akses ke sistem ditolak.

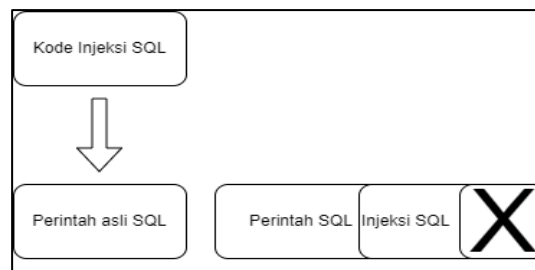
#### II.1.4 Serangan Injeksi SQL (*Structured Query Language*)

Serangan pada database yang termasuk sering ditemukan adalah serangan injeksi SQL. Serangan ini masih masuk dalam daftar 10 besar OWASP (*Open Web Application Security Project*) tahun 2021 tepatnya pada posisi ketiga dimana sebelumnya pernah menduduki posisi pertama pada tahun 2017. Pada tahun 2021 sebanyak 94% aplikasi diuji dalam beberapa bentuk injeksi dengan tingkat kejadian maksimum 19% dan tingkat kejadian rata-rata 3,37% [8].

Serangan injeksi SQL merupakan teknik yang digunakan oleh penyerang dengan mengirimkan perintah SQL melalui URL yang nantinya dieksekusi oleh *web server*. Serangan ini terjadi saat kode SQL jahat diinjeksi ke dalam program database melalui parameter yang selanjutnya dikirimkan ke back-end database server untuk perneksekusiannya [20]. Teknik yang relatif sederhana dan mudah dipahami banyak sumber daya di internet merupakan salah satu karakteristik serangan injeksi SQL. Terjadi masalah dari menggunakan data masukan yang tidak tepercaya hingga

membuat SQL dinamis kueri tanpa verifikasi yang tepat. Penggunaan umum dapat ditemukan kerentanan, penyerang dapat mengekstrak, mengubah, atau menghapus *file* konten dalam *back-end database*. Pernyataan SQL juga memungkinkan penyerang untuk mendapatkan hak administrator pada *database*, sehingga dapat menambah, menyunting, atau menghapus data tanpa ada yang dapat menghentikan penyerang tersebut [21].

Ilustrasi serangan injeksi SQL dapat dilihat pada Gambar II.5 Setelah kode SQL jahat diinjeksikan ke dalam perintah SQL yang asli, maka yang dieksekusi adalah perintah kode SQL jahat.



Gambar II.5 Serangan Injeksi SQL [21]

Beberapa jenis serangan injeksi SQL [22], yakni:

1. Boolean – based blind adalah teknik injeksi yang bergantung pada pengiriman perintah SQL ke database yang memaksa sistem aplikasi untuk mengembalikan hasil yang berbeda.
2. Time – based blind adalah teknik injeksi yang bergantung pada pengiriman perintah SQL ke database yang memaksa database menunggu waktu yang telah ditentukan sebelum merespon, untuk menunjukkan kepada penyerang apakah hasil perintah tersebut benar atau salah.
3. Error based adalah teknik injeksi yang bergantung pada pesan kesalahan yang dikirim oleh database untuk mendapatkan informasi tentang struktur database.
4. UNION – based adalah teknik injeksi yang memanfaatkan operator SQL UNION untuk menggabungkan hasil dari dua atau lebih pernyataan SELECT ke dalam satu hasil yang kemudian dikembalikan sebagai bagian dari respon.
5. Inteferential adalah teknik injeksi yang membutuhkan waktu lebih lama bagi penyerang untuk mengeksploitasi. Penyerang dapat mengubah struktur data dalam database
6. Out – of – band adalah teknik injeksi yang bergantung pada fitur yang diaktifkan pada server database yang digunakan oleh aplikasi web. Teknik ini dapat terjadi ketika penyerang tidak dapat menggunakan saluran yang sama untuk meluncurkan serangan.

### II.1.5 Algoritma Blowfish

Pada proses enkripsi, algoritma kriptografi terdiri atas kunci simetrik dan asimetrik. Menurut Singh [9] mengenai perbandingan algoritma enkripsi menggunakan kunci simetrik dan asimetrik bahwa algoritma enkripsi menggunakan kunci simetrik lebih baik dalam hal kecepatan dan konsumsi daya. Beberapa algoritma enkripsi kunci simetrik menurut Meko [10] yaitu DES, AES, IDEA, dan Blowfish yang memiliki kelebihan dan kekurangan masing-masing dalam proses enkripsi dan dekripsi data yang dilihat dari segi kecepatan maupun keamanan data *ciphertext* yang dihasilkan. Penelitian Diancaraka [11] menyebutkan dari perbandingan algoritma Blowfish dan AES didapatkan hasil enkripsi dan dekripsi Blowfish membutuhkan waktu lebih kecil daripada AES serta *maximum throughput* yang dihasilkan Blowfish lebih tinggi dibandingkan AES. Ini berarti algoritma Blowfish lebih cocok digunakan untuk pengamanan data.

Bruce Schneier merancang algoritma Blowfish menjadi sandi blok kunci simetris pada tahun 1993. Beberapa fitur mencolok dari algoritma Blowfish adalah jadwal kunci yang rumit dan kotak substitusi yang bergantung pada kunci. Algoritma ini memiliki ukuran blok 64 bit dan ukuran kunci mulai dari 32 hingga 448 bit [23]. Algoritma Blowfish digunakan berdasarkan pada penelitian Patel *et al* [23] menyatakan bahwa algoritma Blowfish merupakan algoritma dengan tingkat keamanan dan kecepatan yang tinggi serta belum ada yang bisa mengembangkan serangan yang bisa menembus keamanan dari algoritma Blowfish.

Oleh karena itu, penelitian ini akan menggunakan algoritma Blowfish untuk enkripsi data yang terdapat pada sistem *e-control*.

### II.1.6 Hypertext Preprocessor (PHP) dengan Framework Codeigniter (CI)

*Hypertext Preprocessor* (PHP) merupakan bahasa pemrograman yang populer digunakan untuk membangun sebuah web. PHP tergolong *open source* yang berarti pengembang akan diberikan lisensi tanpa biaya [24]. Seiring berkembangnya teknologi, PHP semakin banyak bermunculan. Hal ini sangat membantu untuk mempermudah dan mempercepat pengembangan web.

*Framework* adalah suatu kerangka kerja yang berupa sekumpulan folder yang memuat *file-file* PHP yang menyediakan *class libraries*, *helpers*, *plugins* dan lainnya. *Framework* menyediakan konfigurasi dan teknik *coding* tertentu. Framework PHP adalah kumpulan fungsi, kelas, dan aturan. Berbagai jenis *framework* PHP telah banyak digunakan dalam pengembangan aplikasi web, misalnya Phalcon, Symfony2, Laravel, CodeIgniter, CakePHP [25].

Pada penelitian [26] melakukan perbandingan antara *framework* CodeIgniter dan *framework* Laravel. Penelitian tersebut menggunakan web server apache xampp.

Kemudian melakukan pengujian *load test* dan *stress test*. Kesimpulan yang didapat yakni dari sisi performansi *framework* CodeIgniter lebih unggul dibandingkan Laravel. Berdasarkan ukuran *page size* pada pengujian *load test*, terdapat kelemahan pada Laravel karena ukuran yang berubah-ubah sehingga CodeIgniter lebih unggul.

Oleh karena hal tersebut penelitian ini akan menggunakan bahasa pemrograman PHP dan berdasarkan perbandingan penelitian [26], penelitian ini akan menggunakan *framework* CodeIgniter karena pengembangan sistem yang besar dan membutuhkan performa baik.

### II.1.7 OWASP Secure Coding Practices Quick Reference Guide

Penerapan *secure coding* dapat mengacu pada OWASP *Secure Coding Practices Quick Reference Guide*. Dokumen ini mendefinisikan serangkaian praktik *secure coding* perangkat lunak umum dengan format daftar periksa yang dapat diintegrasikan ke dalam SDLC. Penerapan praktik ini akan mengurangi kerentanan perangkat lunak yang paling umum [27]. Pada pedoman ini terdapat 14 daftar periksa untuk membantu dalam melakukan pemrograman yang aman. Berikut merupakan daftar periksa yang ada:

1. *Input Validation*
2. *Output Encoding*
3. *Authentication and Password Management*
4. *Session Management*
5. *Access Control*
6. *Cryptographic Practices*
7. *Error Handling and Logging*
8. *Data Protection*
9. *Communication Security*
10. *System Configuration*
11. *Database Security*
12. *File Management*
13. *Memory Management*
14. *General Coding Practices*

Pada penelitian ini akan menggunakan lima daftar periksa yaitu *Input Validation*, *Authentication and Password Management*, *Data Protection*, *Database Security*, dan *File Management* untuk membantu pengamanan sistem dari serangan injeksi SQL.

### II.1.8 Tools SQLMap dan OWASP ZAP (Zed Attack Proxy)

SQLMap adalah aplikasi *open source* atau *tool* yang terdapat dalam Kali Linux. Aplikasi ini digunakan untuk mendeteksi dan mengeksploitasi kerentanan sistem

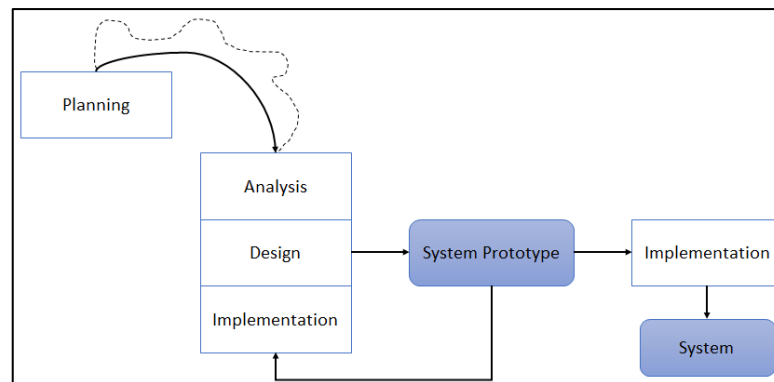
pada web. Aplikasi ini mampu mengambil alih server *database*. Dengan menggunakan SQLMap, penyerang atau *tester* dapat melakukan penyerangan pada *database* SQL, menjalankan perintah pada sistem operasi, mengambil detail struktur *database*, melihat atau menghapus data yang terdapat dalam *database* dan bahkan mengakses sistem *file* dari server [28]. SQLMap mendukung enam teknik injeksi SQL yang sudah dijelaskan di bagian serangan injeksi SQL [22].

Sedangkan OWASP ZAP adalah alat keamanan web gratis yang populer, secara aktif dikelola oleh tim sukarelawan internasional yang berdedikasi. ZAP akan merayapi aplikasi web secara pasif memindai setiap halaman yang ditemukannya. Kemudian ZAP akan menggunakan pemindai aktif untuk menyerang semua halaman yang ditemukan, fungsionalitas, dan parameter. Setelah selesai bekerja, ZAP dapat menampilkan hasil scanning dengan beberapa kategori level resiko (*low*, *medium*, *high*) [29].

Pada penelitian ini akan menggunakan SQLMap dan OWASP ZAP untuk melakukan security testing pada sistem *e-control* tugas akhir dalam mencegah dari serangan injeksi SQL.

### **II.1.9 System Prototyping**

*Prototyping* merupakan salah satu pendekatan yang digunakan pada metodologi pengembangan *System Development Life Cycle* (SDLC) [30]. *Prototyping* diartikan sebagai versi awal dari sistem yang digunakan untuk menjelaskan konsep dan desain secara umum mengetahui lebih lanjut tentang masalah dan kemungkinan solusinya. *Prototyping* diketahui sebagai teknik yang kuat dan digunakan oleh pengembang sistem untuk mendapatkan kebutuhan pemangku kepentingan dari sistem tersebut [31]. Metode ini meliputi empat tahap yaitu *planning*, *analysis*, *design*, dan *implementation*. *System prototyping* akan menghasilkan *prototype* sistem yang diterima oleh pemangku kepentingan dan kemudian diimplementasikan untuk menjadi satu sistem yang utuh [31] [32]. Tahap-tahap penerapan pendekatan ini digambarkan pada Gambar II.6.



Gambar II.6 Tahapan *System Prototyping*

Sumber : telah diolah kembali dari [31]

- a. *Planning*  
Tahap ini memuat inisiasi proyek serta rencana kerja pembangunan sistem sehingga proses pembangunan dapat dijalankan dengan manajemen yang baik.
- b. *Analysis*  
Tahap ini merupakan tindak lanjut dari *system request* untuk diolah menjadi sistem proposal yang berisi hasil analisis kebutuhan fungsional dan nonfungsional, serta deskripsi system bisnis dari system yang akan dibangun.
- c. *Design*  
Pada tahap ini akan dilakukan perancangan sistem aplikasi untuk menentukan bagaimana sistem beroperasi dalam bentuk perangkat lunak. Tahap ini berisi pengembangan *analysis model* menjadi *design models*.
- d. *Implementation*  
Pada tahap ini akan dilakukan pembangunan aplikasi dari tahap perancangan dan pemasangan sistem yang dibangun. Pembangunan aplikasi terdiri dari proses *programming*, *testing* dan *documenting*.
- e. *System Prototype*  
Tahap ini menghasilkan sistem versi sederhana yang diusulkan. Hasil dari tahap ini akan dilakukan evaluasi dan apabila terdapat perubahan akan dilakukan pada tahap akhir.
- f. *System*  
Bagian ini merupakan tahap akhir dari SDLC. Pada tahap ini sistem sudah selesai yang ditandai dengan tidak terdapat perubahan yang dilakukan.

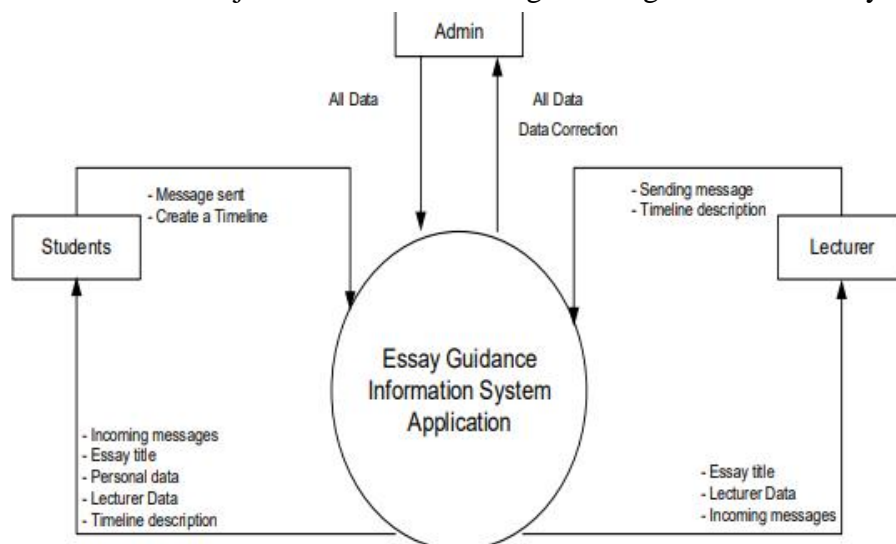
## II.2 PENELITIAN TERKAIT

Berikut merupakan beberapa penelitian terkait dengan penelitian yang akan dilakukan:

### II.2.1 *Online Thesis Guidance Management Information System* [4]

Penelitian ini dilakukan oleh Nasution, Pratama, Tanjung, Siregar, dan Amalia. Permasalahan dari penelitian adalah perkembangan teknologi dalam dunia Pendidikan masih belum maksimal, terutama dalam proses bimbingan tugas akhir antara mahasiswa dan dosen. Kesulitan dosen yakni keterbatasan waktu komunikasi dan kesesuaian jadwal antara mahasiswa dan dosen.

Untuk mengatasi masalah tersebut, penelitian ini memberikan solusi perancangan sistem informasi manajemen bimbingan tugas akhir *online* yang membantu mahasiswa dan dosen untuk melakukan proses bimbingan tanpa batas ruang dan waktu. Sistem terdiri dari aplikasi admin berbasis web dan berbasis Android untuk mahasiswa dan dosen. Terdapat tiga aktor di dalamnya, yakni mahasiswa, dosen, dan admin. Berikut disajikan Gambar II.7 mengenai diagram alur bisnisnya.



Gambar II.7 Alur bisnis penelitian [4]

### II.2.2 *Sistem Aplikasi Pengelolaan Tugas Akhir Berbasis Mobile* [3]

Penelitian ini dilakukan oleh Julianto Simatupang dan Muhammad. Permasalahan yang diangkat pada masalah ini, banyaknya prosedur administratif yang harus dilakukan oleh mahasiswa dan proses pengajuan tugas akhir yang masih manual sehingga mengakibatkan program studi mengalami kesulitan dalam pengelolaan tugas akhir. Misalnya seperti proses penyajian informasi yang membutuhkan waktu yang lama karena harus menghitung satu per satu lembar pengajuan judul yang masuk dan membuat pengumuman hasil seleksi judul melalui majalah dinding



kampus. Hal ini kurang efektif dan efisien sehingga diusulkan penerapan teknologi dalam pengelolaan tugas akhir.

Oleh karena itu pengembangan sistem aplikasi menjadi solusi untuk pengelolaan tugas akhir sehingga dapat mempermudah mengkordinir dan mengelola tugas akhir. Fitur-fitur yang terdapat di dalamnya yakni inputan data mahasiswa, data jadwal, dan form pengajuan judul. Mahasiswa kapan dan dimana saja dapat mengakses dan melihat informasi terkait tugas akhir dari *smartphone* mereka tanpa batas waktu dan jarak.

### **II.2.3 An Improved OTP Grid Authentication Scheme Email-based using Middle-square for Disaster Management System [18]**

Penelitian ini dilakukan oleh Balilo, Gerardo, Medina, dan Byung. Permasalahan dari penelitian adalah adanya bencana yang berupaya untuk mengontrol atau mengakses sistem tanpa izin yang sah/sah dan protokol otorisasi yang tepat dari entitas yang sah. Terdapat autentikasi berbasis email *one time password* (OTP) dan meningkatkan skema autentikasi menggunakan teknik *middle square* untuk melindungi dan mengamankan informasi rahasia untuk sistem manajemen bencana.

Penelitian ini berhasil meningkatkan tingkat keamanan, perlindungan, dan kepercayaan pengguna karena menggunakan *random generator* kode OTP yang dikirim melalui akun email aman yang bebas dari *brute force*, *dictionary attack*, *insider attack*, dan *key-logger attacks*.

### **II.2.4 Perbandingan Algoritma AES dan Blowfish untuk Pengamanan Data dalam Database pada Rancang Bangun Aplikasi Pengelolaan Surat berbasis Web Dinas Pendidikan Kota Mataram [11]**

Penelitian ini dilakukan oleh Pandu Bagus Diancaraka. Permasalahan dari penelitian adalah adanya pengelolaan surat pada Dinas Pendidikan Kota Mataram masih bersifat manual menggunakan buku agenda yang diganti setiap tahun yang menyebabkan surat rentan hilang maupun rusak, memerlukan tempat penyimpanan buku agenda atau data surat lainnya. Kemudian Dinas Pendidikan Kota Mataram juga memiliki *bandwidth* hanya sebesar 24mbps. Untuk itu, perlu menemukan algoritma yang tepat untuk mendukung pengamanan data aplikasi yang akan dibangun tersebut dengan membandingkan algoritma AES dan Blowfish.

Untuk mengatasi masalah tersebut, penelitian ini memberikan solusi perancangan Aplikasi Pengelolaan Surat berbasis Web dengan hasil algoritma Blowfish lebih cocok digunakan dari segi kecepatan enkripsi, dekripsi, dan *maximal Throughput*.

Berikut memuat perbandingan penelitian yang terkait.

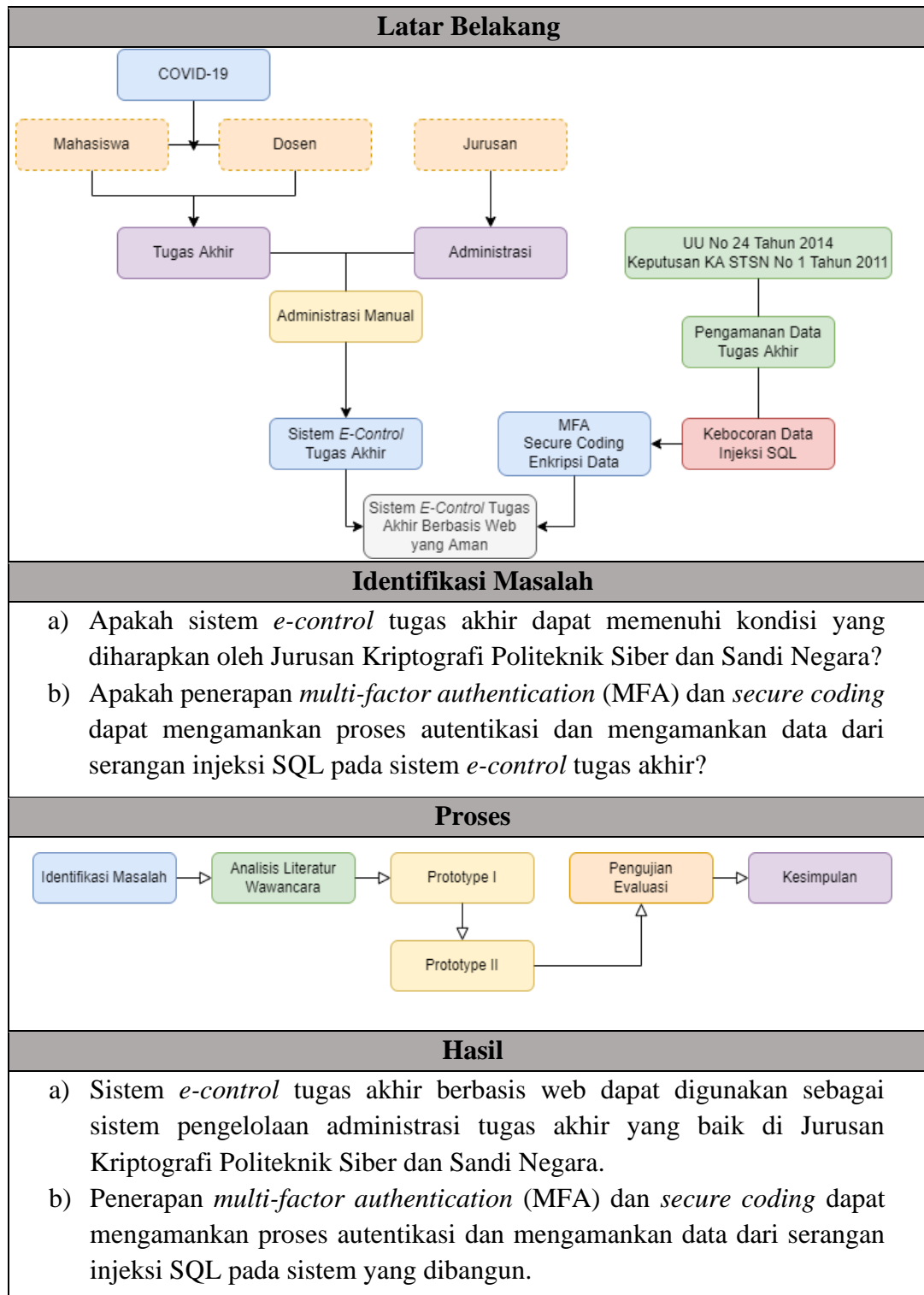
Tabel II.2 Perbandingan Penelitian Terkait

No	Judul Penelitian	Tahun	Hasil	Proses yang diambil
1.	<i>Online Thesis Guidance Management Information System</i>	2018	<ul style="list-style-type: none"> <li>- Aktor-aktornya adalah mahasiswa, dosen, admin</li> <li>- Bimbingan ditekankan pada komunikasi sistem antara mahasiswa dan dosen</li> <li>- Tidak membahas keamanan data</li> </ul>	Proses bimbingan menggunakan sistem
2.	Sistem Aplikasi Pengelolaan Tugas Akhir Berbasis <i>Mobile</i>	2019	<ul style="list-style-type: none"> <li>- Tidak menjelaskan aktor dan alur bisnis</li> <li>- Fitur yang dapat digunakan adalah inputan data mahasiswa, data jadwal, dan form pengajuan judul</li> <li>- Tidak membahas keamanan data</li> </ul>	Beberapa fitur dalam pengelolaan tugas akhir
3.	<i>An Improved OTP Grid Authentication Scheme Email-based using Middle-square for Disaster Management System</i>	2017	<ul style="list-style-type: none"> <li>- Perbaikan pada skema OTP menjadi lebih kompleks dapat mencegah <i>brute force</i> dan <i>dictionary attack</i></li> <li>- Algoritma ini memiliki keunggulan dibandingkan autentikasi tradisional dan skema cetak OTP</li> </ul>	Penggunaan kode OTP menggunakan <i>email</i> sebagai pendukung MFA
4.	Perbandingan Algoritma AES dan Blowfish untuk Pengamanan Data dalam <i>Database</i> pada Rancang Bangun Aplikasi Pengelolaan Surat berbasis Web Dinas Pendidikan Kota Mataram	2021	<ul style="list-style-type: none"> <li>- Pengamanan <i>database</i> dan penerapan enkripsi dapat mengurangi dampak serangan injeksi SQL</li> <li>- Algoritma Blowfish lebih sesuai digunakan pada sistem aplikasi dari segi waktu enkripsi dan dekripsi dan <i>maximum throughput</i> yang dihasilkan</li> </ul>	Penggunaan algoritma Blowfish untuk pengamanan data

### II.3 KERANGKA/MODEL KONSEPTUAL

Kerangka/model mengenai hubungan setiap konsep yang akan diteliti pada penelitian ini dapat dilihat pada Tabel II.2 sebagai berikut:

Tabel II.3 Kerangka Konseptual



## **BAB III METODOLOGI PENELITIAN**

### **III.1 OBJEK PENELITIAN**

Jurusan Kriptografi merupakan unsur pelaksana pendidikan di Politeknik Siber dan Sandi Negara (Poltek SSN). Jurusan mempunyai tugas melaksanakan pendidikan vokasi dalam satu atau beberapa cabang ilmu pengetahuan dan/atau teknologi serta pengelolaan sumber daya pendukung program studi [16]. Salah satu pengelolaannya yakni mengelola tugas akhir mahasiswa tingkat akhir. Mengikuti perkembangan teknologi menjadikan kebutuhan perangkat atau sistem yang memudahkan jurusan mengelola dan memonitor mahasiswa dan dosen dalam menyelesaikan tugas akhir.

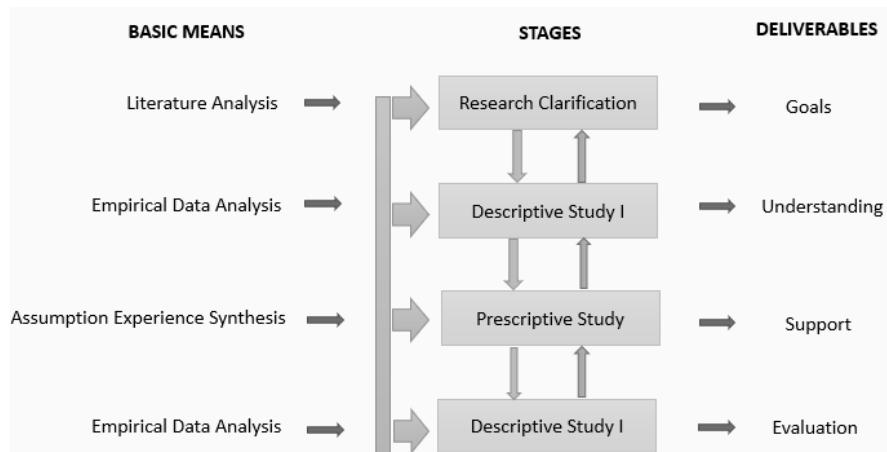
Pada penelitian ini akan merancang dan membangun sistem *e-control* tugas akhir pada Jurusan Kriptografi Poltek SSN sebagai alternatif untuk mengelola tugas akhir mahasiswa yang sekaligus menjadi objek penelitian.

### **III.2 JENIS PENELITIAN**

Metode yang digunakan dalam penelitian ini adalah kualitatif. Metode kualitatif sering disebut penelitian naturalistik karena penelitiannya dilakukan pada kondisi yang alamiah serta teknik pengumpulan data yang dilakukan bersifat triangulasi, yaitu menggunakan berbagai teknik pengumpulan data secara gabungan/simultan. Pendekatan kualitatif digunakan juga ketika pengembangan sistem mengumpulkan data dengan melakukan *in-depth interview* (wawancara) sehingga ada interaksi antara peneliti data dengan sumber data serta hasil dari pengumpulan data tersebut disajikan berupa tabel [33].

### **III.3 DESAIN PENELITIAN**

Metode penelitian ini akan menggunakan *Design Research Methodology* (DRM). DRM terdiri dari empat tahapan yaitu *Research Clarification*, *Descriptive Study I*, *Prescriptive Study* dan *Descriptive Study II*. Pada tahap *Prescriptive Study* akan diterapkan tahapan metode pengembangan perangkat lunak *Software Prototyping* sebagai solusi permasalahan penelitian. Tahap-tahap digambarkan pada Gambar III.1.

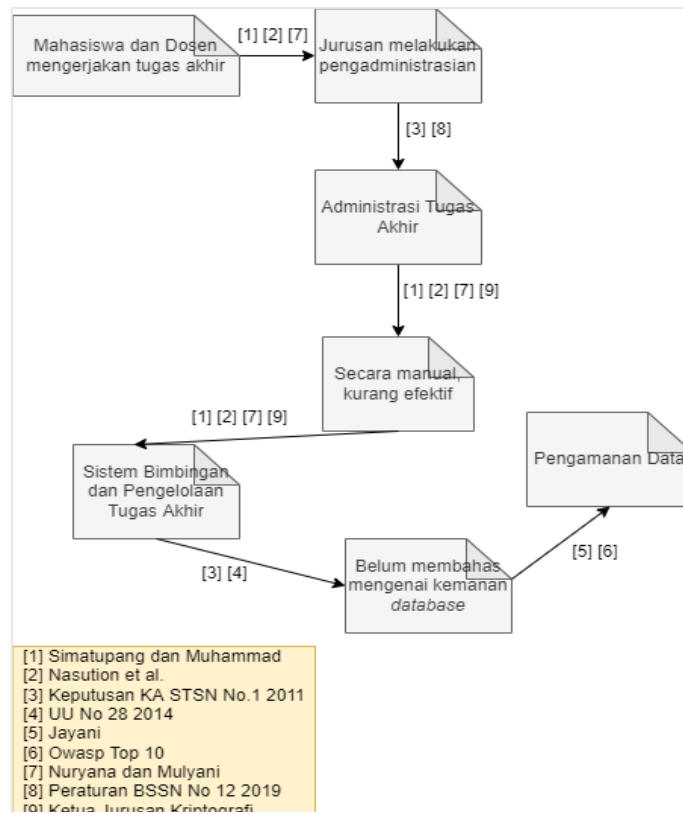


Gambar III.1 Skema *Design Research Methodology*

Sumber : telah diolah kembali dari [30]

### III.3.1 Research Clarification (RC)

*Research Clarification* merupakan tahap untuk mengumpulkan bukti dan teori yang mendukung penelitian [17]. Kumpulan bukti dan teori berdasarkan telaah kepustakaan dan wawancara untuk mendukung penelitian. Kepustakaan yang dikumpulkan berisi tentang masalah yang terdapat pada penerapan sistem *e-control* tugas akhir dan solusi yang ditawarkan untuk mengatasi masalah tersebut. Wawancara digunakan untuk mengetahui permasalahan pada lokus yang dijadikan acuan untuk penelitian.



Gambar III.2 Skema Studi Literatur

Salah satu tugas dari Jurusan Kriptografi yakni melakukan administrasi pada tugas akhir mahasiswa di Poltek SSN [5]. Pengelolaan tugas akhir masih menggunakan metode manual yaitu dengan mengirimkan tautan pendaftaran maupun pengumpulan tugas akhir kepada mahasiswa dan dosen secara langsung. Hal tersebut menimbulkan masalah yaitu lamanya waktu dan sering terjadi keterlambatan dalam pengumpulan laporan perkembangan. Kemudian juga proses kontrol bimbingan yang tidak bisa dipantau oleh jurusan secara langsung, ada juga ketidaklengkapan dan ketidaksesuaian *file* yang seharusnya dikumpulkan oleh mahasiswa berdasarkan wawancara dengan Ketua Jurusan Kriptografi Poltek SSN.

Permasalahan tersebut dapat diatasi dengan melakukan pembuatan sistem atau aplikasi pengelolaan tugas akhir [3] [4] [15] namun ketiga penelitian tersebut belum membahas tentang keamanan sistem atau *database* yang seharusnya diamankan sesuai UU Nomor 24 Tahun 2014 tentang Hak Cipta. Diperlukan pengamanan data sebagai langkah preventif data tersebut digunakan oleh pihak yang tidak berkepentingan sehingga diterapkan juga algoritma yang melindungi data.

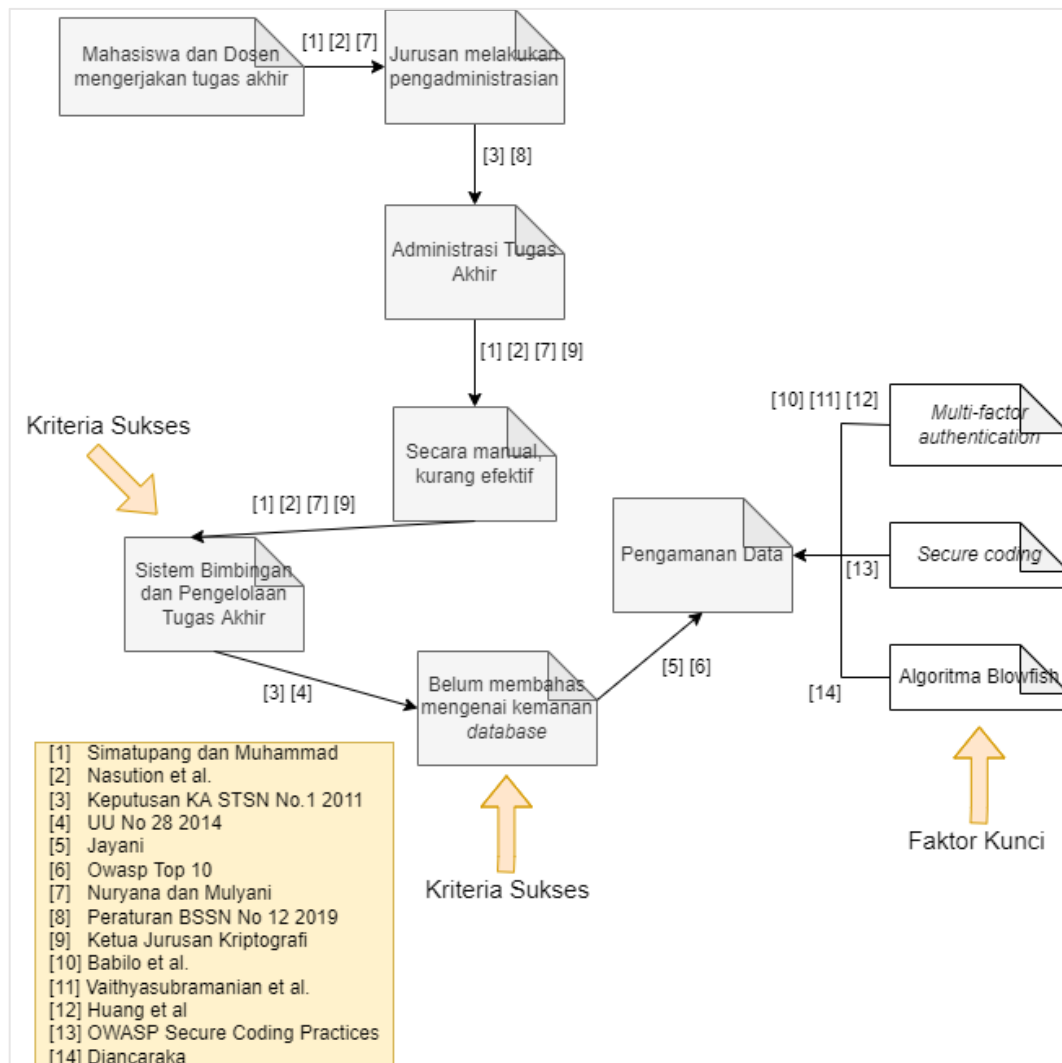
Berdasarkan studi literatur, didapatkan tujuan yang menjadi fokus dari penelitian yaitu apakah penerapan *multifactor authentication* dan *secure coding* dapat memberi keamanan *database* pada sistem dari serangan injeksi SQL. Hal ini berdasarkan permasalahan yang didapatkan yaitu belum terpenuhinya sistem yang harus melindungi data pribadi dan data tugas akhir mahasiswa.

### III.3.2 Descriptive Study I (DS I)

Pada *Descriptive Study* akan dilakukan analisis literatur yang bersifat lanjutan berdasarkan dari referensi yang digunakan dengan penelitian yang akan dikerjakan. Kemudian juga akan terdapat desain penelitian yang disebut model referensi berdasarkan pertimbangan-pertimbangan yang telah didapatkan dari proses sebelumnya pada RC [30]. Penjelasan mengenai tahap ini terdapat pada Gambar III.3. Berikut didapatkan hal yang menentukan keberhasilan tujuan penelitian, yaitu:

- a. Faktor Kunci merupakan faktor utama yang mempengaruhi faktor lain untuk mencapai kriteria sukses. Faktor kunci pada penelitian ini adalah rancang bangun sistem *e-control* tugas akhir yang sesuai dengan kebutuhan lokus dan melakukan pengamanan *database* dari serangan injeksi SQL.
- b. Kriteria Sukses merupakan kondisi yang harus dicapai untuk memenuhi tujuan penelitian. Pada penelitian ini kriteria sukses dibuktikan dengan dihasilkannya sistem kontrol tugas akhir yang aman dengan menerapkan

*multi-factor authentication, secure coding, dan algoritma Blowfish untuk enkripsi data.*



Gambar III.3 Model Referensi

### III.3.3 Prescriptive Study (PS)

Pada *Prescriptive Study* akan dilakukan penyelesaian masalah dengan melakukan rancang bangun aplikasi atau sistem [30]. Proses rancang bangun akan menerapkan metode pengembangan perangkat lunak dengan pendekatan *system prototyping*. Berikut akan dijelaskan tahapan metode *software prototyping* pada Tabel III.1.

Tabel III.1 Tahapan Perancangan dan Pengembangan Aplikasi

Tahap	Input	Proses	Output
<i>Planning</i>	-	<ul style="list-style-type: none"> <li>- Mempelajari penelitian terkait</li> <li>- Mencari referensi penelitian terkait</li> </ul>	Proposal penelitian

		<ul style="list-style-type: none"> <li>- Penyusunan proposal</li> </ul>	
<i>Analysis</i>	Proposal penelitian	<ul style="list-style-type: none"> <li>- Melakukan wawancara dengan narasumber dari Jurusan Kriptografi Poltek SSN</li> <li>- Membuat penjelasan rinci mengenai kebutuhan sistem dengan mencari aplikasi serupa</li> </ul>	<ul style="list-style-type: none"> <li>- Kebutuhan fungsional</li> <li>- Kebutuhan non-fungsional</li> </ul>
<i>Design</i>	<ul style="list-style-type: none"> <li>- Kebutuhan fungsional</li> <li>- Kebutuhan non-fungsional</li> </ul>	Membuat perancangan sistem aplikasi menggunakan <i>Unified Modelling Language</i> (UML)	<ul style="list-style-type: none"> <li>- <i>Use case diagram</i></li> <li>- <i>Class diagram</i></li> <li>- <i>Sequence diagram</i></li> <li>- <i>Activity diagram</i></li> <li>- <i>Entity Relationship Diagram</i></li> </ul>
<i>Implementation I</i>	<ul style="list-style-type: none"> <li>- <i>Use case diagram</i></li> <li>- <i>Class diagram</i></li> <li>- <i>Sequence diagram</i></li> <li>- <i>Activity diagram</i></li> <li>- <i>Entity Relationship Diagram</i></li> </ul>	<ul style="list-style-type: none"> <li>- Membuat <i>prototype</i> sistem</li> <li>- Pengujian terhadap sistem</li> </ul>	<ul style="list-style-type: none"> <li>- Sistem aplikasi <i>prototype I</i></li> <li>- Hasil analisis pengujian sistem aplikasi</li> </ul>
<i>Implementation II</i>	<ul style="list-style-type: none"> <li>- Hasil analisis pengujian sistem aplikasi</li> <li>- Sistem aplikasi <i>prototype I</i></li> </ul>	<ul style="list-style-type: none"> <li>- Membuat <i>prototype</i> sistem berdasarkan hasil analisis pengujian sistem sebelumnya</li> <li>- Pengujian terhadap sistem aplikasi</li> </ul>	<ul style="list-style-type: none"> <li>- Sistem aplikasi <i>prototype II</i></li> <li>- Hasil analisis pengujian sistem aplikasi</li> </ul>

a. *Planning*



Pada *planning* akan dilakukan inisiasi pada proses rancang bangun, yaitu melakukan deskripsi pada sistem. Deskripsi sistem ini digunakan untuk menjelaskan lebih luas tentang aplikasi yang akan dibangun.

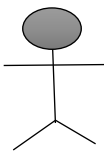


b. *Analysis*


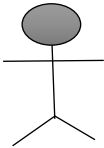

Pada *analysis* akan dilakukan analisis kebutuhan fungsional dan non-fungsional. Hasil dari analisis ini adalah analisis fungsi dan fitur apa saja yang harus ada di aplikasi.







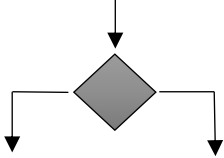

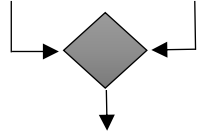
c. *Design*

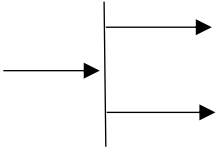
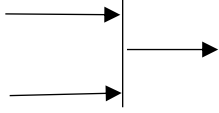
Pada tahap ini akan membuat rancangan system menggunakan UML dan *Entity Relationship Diagram*. Berdasarkan [32], sekarang ini yang menjadi standarisasi analisis dan perancangan sistem berorientasi objek adalah bahasa pemodelan UML. Namun UML hanya berisi diagram-diagram dan notasi-notasi, tidak menjelaskan mengenai kerangka kerja dalam proses rekayasa perangkat lunak. Oleh karena itu, ada beberapa jenis UML yang harus dijelaskan dalam penelitian ini guna mengetahui tingkah laku dinamis dari objek-objek dalam aplikasi, yang mana bisa dijelaskan sebagai sederet perubahan-perubahan dalam aplikasi sepanjang waktu. Diantaranya *use case diagram*, *activity diagram*, *sequence diagram*, dan *class diagram*. *Use case diagram* akan menyajikan apa saja yang dapat dilakukan oleh pengguna dan aplikasi. *Class diagram* akan menggambarkan model statis yang mendukung tampilan statis dari sistem yang berkembang. *Sequence diagram* menggambarkan objek yang terlibat dalam *use case* pada aplikasi. *Activity diagram* merupakan model dinamis yang bekerja pada sistem.

Tabel III.2 Atribut Diagram UML

No	Simbol	Keterangan	Jenis
1.	 <i>Actor</i>	Merupakan seseorang atau sistem yang memperoleh keuntungan dari dan di luar sistem. Simbol ini diletakkan di luar batasan sistem.	<i>Use Case Diagram</i>
2.	 <i>Use Case</i>	Merupakan bagian utama dari fungsi pada sistem. Simbol ini diletakkan di dalam batasan sistem.	
3.	 <i>System Boundary</i>	Merepresentasikan cakupan dari sistem. Penempatan nama sistem dapat di atas maupun di dalam.	

4.	 <i>Association relationship</i>	Menghubungkan aktor dengan <i>use case</i> .	
5.	<div style="background-color: #cccccc; padding: 2px; text-align: center;">Nama Class</div> <div style="text-align: center;">-Attribute -/derived attribute name</div> <hr style="width: 100%;"/> <div style="text-align: center;">+operation name() Class</div>	Menggambarkan mengenai orang, tempat atau benda dimana sistem harus menangkap dan menyimpan informasinya.	<i>Class Diagram</i>
6.	<div style="text-align: center;">- Attribute name - /derived attribute name  Attribute</div>	Merupakan properti yang menggambarkan keadaan dari suatu objek.	
7.	<div style="text-align: center;">+ Operation name()  Method</div>	Merupakan aksi atau fungsi yang dijalankan oleh kelas.	
8.	<div style="text-align: center;">1..*    Verb phrase    0..1</div> <hr style="width: 100%;"/> <div style="text-align: center;">Association</div>	Merupakan relasi antara beberapa kelas atau sebuah kelas dengan dirinya sendiri.	
9.	 <i>Actor</i>	Merupakan seseorang atau sistem yang memperoleh keuntungan dari dan di luar sistem. Simbol ini diletakkan di atas diagram.	<i>Sequence Diagram</i>
10.	<div style="background-color: #cccccc; padding: 5px; text-align: center;"> <u>anObject:aClass</u> </div> <div style="text-align: center;">Object</div>	Berperan secara berurutan dengan mengirimkan dan atau menerima pesan.	
11.	<div style="text-align: center;">   Life Line </div>	Menunjukkan objek yang sedang aktif dalam sebuah urutan.	

12.	 <i>Focus of Control</i>	Menunjukkan kapan sebuah objek menerima maupun mengirim pesan.	
13.	 <i>Message</i>	Menyampaikan informasi dari satu objek ke objek lain.	
14.	 <i>Object Destruction</i>	Ditempatkan di akhir objek <i>lifeline</i> untuk menunjukkan bahwa objek ini berakhir.	
15.	 <i>Activity</i>	Menggambarkan pekerjaan yang dilakukan pada aliran kerja.	<i>Activity Diagram</i>
16.	 <i>Initial State</i>	Menggambarkan titik dimana dimulainya aliran kerja <i>activity diagram</i>	
18.	 <i>Final State</i>	Menggambarkan bagian akhir aliran kerja <i>activity diagram</i>	
19.	 <i>Decision</i>	Menggambarkan pilihan kondisi dimana ada kemungkinan perbedaan transisi	
20.	 <i>Transition</i>	Menghubungkan aktivitas sebelumnya dengan aktivitas selanjutnya.	
21.	 <i>Merge</i>	Menggabungkan kembali aliran kerja yang dipecah <i>decision</i>	

22	 <i>Synchronization Fork</i>	Memecah <i>behavior</i> menjadi aktivitas paralel	
23	 <i>Synchronization Join</i>	Menggabungkan kembali aktivitas yang paralel	

d. *Implementation I*

Tahap selanjutnya yakni pembangunan sistem aplikasi *prototype I* akan dilakukan implementasi ke dalam *source code* dengan bahasa PHP. Sistem *e-control* pada tahap ini memastikan *user requirement* sudah terpenuhi. Kemudian juga akan dilakukan pengujian user acceptance test (UAT).

e. *Implementation II*

Pada tahap ini dilakukan pembangunan sistem aplikasi *prototype II* dengan menambahkan fitur keamanan yakni MFA dan *secure coding* untuk menjawab rumusan masalah pada penelitian ini.

### III.3.4 Descriptive Study II (DS II)

Pada tahap ini akan dilakukan pengujian tahap akhir pada sistem aplikasi yang utuh. Pengujian ini ditujukan untuk membuktikan bahwa sistem yang dibangun telah memenuhi kriteria sukses penelitian. Berdasarkan penelitian Kundu [34] dapat dilakukan modifikasi dengan menyesuaikan kebutuhan, pengujian sistem aplikasi yang akan dilakukan yaitu *user acceptance test* (UAT), *usability testing*, dan *security testing*.

a. *User Acceptance Test* (UAT)

Dalam pengujian ini akan dilakukan penyebaran kuesioner yang berisi pertanyaan-pertanyaan berkaitan dengan tampilan dan fungsi dari sistem aplikasi apakah sudah sesuai dengan kebutuhan pengguna. Tujuan dari kuesioner ini yaitu mengumpulkan tanggapan pengguna dan sebagai konfirmasi apakah sistem aplikasi sudah sesuai dengan kebutuhan. Penilaian menggunakan skala Guttman yang merupakan skala pengukuran yang membutuhkan jawaban tegas dari responden, misal “benar” atau “salah”, “ya” atau “tidak”, “pernah” atau “tidak pernah”. Pada intinya, jawaban hanya ya atau tidak dengan pemberian skor jika ya artinya 1 dan jika tidak

artinya 0, lalu akan dicari rata-rata nilai dari jumlah jawaban yang diberikan oleh responden.

*b. Usability Testing*

Dalam pengujian ini dilakukan untuk menguji fungsi dari fitur-fitur seperti tautan dan tombol dari sistem atau sering disebut *navigation testing*. Acuan pengujian ini yakni *functional testing* yang sejalan dengan pengujian tautan dan tombol. Hasil dari pengujian berupa keterangan “*Pass*” jika hasil pengujian sesuai harapan dan “*Fail*” jika hasil pengujian tidak sesuai harapan.

*c. Security Testing*

Dalam pengujian ini dilakukan untuk memastikan keamanan data pada *database* sistem dengan melakukan Injeksi SQL menggunakan *tools* berupa sqlmap dan OWASP ZAP. Pengujian yang akan dilakukan sebagai berikut:

- Melakukan pengujian menggunakan *tools* sqlmap untuk mendapatkan *database* pada sistem.
- Melakukan pengujian menggunakan *tools* OWASP ZAP untuk mengetahui kerentanan yang terdapat pada sistem.

Dalam pengujian ini dilakukan sekaligus menjawab rumusan masalah yang sudah ditentukan serta membantu menemukan kekurangan bahkan kesalahan pada sistem *e-control* ini.



## DAFTAR PUSTAKA

- [1] N. Makariem, "Pelaksanaan Kebijakan Pendidikan dalam Masa Darurat Penyebaran Corona Virus Disease (Covid 19)." Surat Edaran Nomor 4 Tahun 2020, Mar. 24, 2020.
- [2] Nizam, "Penyelenggaraan Pembelajaran Tatap Muka Tahun Akademik 2021/2022." Surat Edaran Nomor 4 Tahun 2021, 2021.
- [3] J. Simatupang and M. Muhammad, "Sistem Aplikasi Pengelolaan Tugas Akhir Berbasis Mobile," *IT J. Res. Dev.*, vol. 3, no. 2, pp. 66–75, Feb. 2019, doi: 10.25299/itjrd.2019.vol3(2).2339.
- [4] T. H. Nasution, F. Pratama, K. Tanjung, I. Siregar, and A. Amalia, "Online thesis guidance management information system," *J. Phys. Conf. Ser.*, vol. 978, p. 012081, Mar. 2018, doi: 10.1088/1742-6596/978/1/012081.
- [5] P. Tugas Akhir, "Keputusan Ketua Sekolah Tinggi Sandi Negara No.001 Tahun 2011 Tentang Pedoman Tugas Akhir".
- [6] H. Cipta, "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 28 TAHUN 2014 TENTANG," p. 84.
- [7] D. H. Jayani, "Pencurian Data Pribadi Makin Marak Kala Pandemi," *Databoks*, 2021. [Online]. Available: <https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi>
- [8] "Owasp Top 10," 2021. [Online]. Available: <https://owasp.org/Top10/>
- [9] P. Sharma and D. Singh, "Comparative Study of Various SDLC Models on Different Parameters," *Int. J. Eng. Res.*, vol. 4, no. 4, pp. 188–191, Apr. 2015, doi: 10.17950/ijer/v4s4/405.
- [10] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *J. Teknol. Terpadu*, vol. 4, 2018.
- [11] P. B. Diancaraka, "Perbandingan Algoritma AES dan Blowfish untuk Pengamanan Data dalam Database pada Rancang Bangun Aplikasi Pengelolaan Surat berbasis Web Dinas Pendidikan Kota Mataram," *Politek. Siber Dan Sandi Negara*, 2021.
- [12] E. Ribeiro de Mello *et al.*, "Multi-factor authentication for shibboleth identity providers," *J. Internet Serv. Appl.*, vol. 11, no. 1, p. 8, Dec. 2020, doi: 10.1186/s13174-020-00128-1.
- [13] S. Vaithyasubramanian, A. Christy, and D. Saravanan, "Two Factor Authentications For Secured Login In Support of Effective Information Preservation and Network Security," vol. 10, no. 5, p. 5, 2015.
- [14] Y. Huang, Z. Huang, H. Zhao, and X. Lai, "A new One-time Password Method," *IERI Procedia*, vol. 4, pp. 32–37, 2013, doi: 10.1016/j.ieri.2013.11.006.
- [15] Y. Nuryana and A. Mulyani, "Pengembangan Aplikasi Pengendalian Skripsi Berbasis Android Untuk Mahasiswa Dan Dosen," *J. Algoritma*, vol. 14, no. 2, pp. 187–192, Feb. 2015, doi: 10.33364/algoritma/v.14-2.187.
- [16] BSSN, "Peraturan Badan Siber dan Sandi Negara Nomor 12 Tahun 2019 tentang Organisasi dan Tata Kerja Politeknik Siber Dan Sandi Negara," 2019.
- [17] R. Allen and A. Pickup, "Two-Factor Authentication," in *Digital Identity Management*, 1st edition., vol. 6, 2007.

- [18] B. B. Jr. Balilo, B. D. Gerardo, R. P. Medina, and Y. Byung, "An Improved OTP Grid Authentication Scheme Email-based using Middle-square for Disaster Management System," *Int. J. Grid Distrib. Comput.*, vol. 10, no. 11, pp. 43–56, Nov. 2017, doi: 10.14257/ijgdc.2017.10.11.05.
- [19] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, T.-H. Kim, and H. Elkamchouchi, "Mobile one-time passwords two-factor authentication using mobile phones," 2011.
- [20] Bangkit Wiguna, W. Adi Prabowo, and R. Ananda, "Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website," *Digit. Zone J. Teknol. Inf. Dan Komun.*, vol. 11, no. 2, pp. 245–256, Nov. 2020, doi: 10.31849/digitalzone.v11i2.4867.
- [21] \* P., A. Sunyoto, and E. Pramono, "Deteksi Serangan SQL Injection Menggunakan Hidden Markov Model," *J. TECNOSCIENZA*, vol. 5, no. 2, p. 243, Apr. 2021, doi: 10.51158/tecnoscienza.v5i2.432.
- [22] S. Lika, R. D. P. Halim, and I. Verdian, "Analisa Serangan SQL Injeksi Menggunakan SQLMap," vol. 4, p. 7, 2018.
- [23] P. Patel, R. Patel, and N. Patel, "Integrated ECC and Blowfish for Smartphone Security," *Procedia Comput. Sci.*, vol. 78, pp. 210–216, 2016, doi: 10.1016/j.procs.2016.02.035.
- [24] K. Ahmad, J. Shekhar, and K. P. Yadav, "Classification of SQL Injection Attacks," p. 9, 2010.
- [25] M. I. N. Saroni and B. Mulyanti, "Hypertext preprocessor framework in the development of web applications," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 830, no. 2, p. 022096, Apr. 2020, doi: 10.1088/1757-899X/830/2/022096.
- [26] R. Erinton, R. M. Negara, and D. D. Sanjoyo, "Analisis Performansi Framework CodeIgniter dan Laravel Menggunakan Web Server Apache," p. 8.
- [27] K. Turpin, "Secure Coding Practices - Quick Reference Guide," p. 17, 2010.
- [28] B. S. Samantha and M. V. Phanindra, "An Overview on the Utilization of Kali Linux Tools," vol. 5, no. 2, p. 10.
- [29] D. W., "Zed Attack Proxy (ZAP)." OWASP, 2020.
- [30] L. T. M. Blessing and A. Chakrabarti, *DRM, a Design Research Methodology*. London: Springer London, 2009. doi: 10.1007/978-1-84882-587-1.
- [31] S. B., "Software Prototypes: Enhancing The Quality of Requirements Engineering Process," *2015 Int. Symposium Technol. Manag. Emerg. Technol. ISMET*, 2015.
- [32] A. Dennis, B. Wixom, and R. Roth, *System Analysis and Design*, 5th ed. 2012.
- [33] Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif, dan R&D," *Bdg. Alf.*, 2013.
- [34] S. Kundu, "Web Testing: Tool, Challenges and Methods," vol. 9, no. 2, p. 6, 2012.



## **LAMPIRAN**

**Lampiran 1 Transkrip Wawancara  
Tahap Penelitian**

TRANSKRIP WAWANCARA

**Rancang Bangun Sistem *E-Control* Tugas Akhir pada Jurusan Kriptografi  
Politeknik Siber dan Sandi Negara**

Nama : Dion Ogi, S.Pd., M.T.  
Jabatan : Ketua Jurusan Kriptografi  
Unit Kerja : Politeknik Siber dan Sandi Negara  
Hari/Tanggal : Jumat/17 Desember 2021

---

1. Apakah sistem pengelolaan tugas akhir sedang dibutuhkan oleh Jurusan Kriptografi Poltek SSN? Jika iya, mengapa?

**Jawaban :**

Ya, untuk mengatasi permasalahan-permasalahan yang ada dalam pengelolaan tugas akhir secara manual saat ini.

2. Apa kendala-kendala pada pengelolaan tugas akhir saat ini dan diharapkan dapat diselesaikan dengan sistem ini?

**Jawaban :**

Masalah keterlambatan pengumpulan *progress*, Ketidaklengkapan dan ketidaksesuaian file yang dikumpulkan, Tidak bisa kontrol bimbingan langsung kepada mahasiswa dan dosen.

3. Apakah adanya pandemi COVID-19 mempengaruhi atau menghambat proses pengerjaan tugas akhir?

**Jawaban :**

Tidak terlalu berpengaruh kecuali tidak ada fasilitas komunikasi antara mahasiswa dan dosen. Sekarang sudah ada platform komunikasi *online*.

4. Sistem yang dibutuhkan lebih baik android atau web? Mengapa?

**Jawaban :**

Lebih baik web karena aksesibilitasnya lebih luas dibandingkan android.

5. Apa saja aktor yang dibutuhkan dalam sistem?

**Jawaban :**

Mahasiswa, dosen, jurusan, prodi.

6. Bagaimana alur bisnis pengelolaan tugas akhir di Jurusan Kriptografi?

**Jawaban :**

Memiliki alur yang cukup banyak, terdapat pada *file* yang sudah saya berikan.

7. Apa saja fitur-fitur yang dibutuhkan oleh Jurusan Kriptografi dalam mengelola tugas akhir?

**Jawaban :**

Jurusan dapat memantau dosen dan mahasiswa, Dosen dapat memantau mahasiswa, Fitur pengingat/reminder untuk mahasiswa dan dosen, Laporan setiap perkembangan tugas akhir, dll menyesuaikan kebutuhan sesuai proses bisnis.

Bogor, 26 Desember 2021

Mengetahui,



Dion Ogi, S.Pd., M.T.

NIP. 19791206 199911 1 001

## Lampiran 2 User Acceptance Test

### KUISIONER PENILAIAN SISTEM *E-CONTROL* TUGAS AKHIR

#### Petunjuk Pengisian Kuisisioner

1. Dimohon dengan hormat bantuan dan kesediaan Bapak/Ibu dan Rekan-rekan untuk menanggapi seluruh pertanyaan sesuai dengan posisi/jabatan masing-masing.
2. Bapak/Ibu dan Rekan-rekan dipersilahkan memilih tanggapan yang sesuai dengan kondisi yang dihadapi saat melakukan uji coba sistem dengan cara memilih satu jawaban yakni **Ya** atau **Tidak** dengan memberikan tanda checklist (√).
3. Jika terjadi perubahan jawaban ke jawaban lainnya, pada jawaban yang tidak digunakan dapat dibubuhkan tanda sama dengan (=).

Atas perhatian dan kesediaan untuk mengisi angket ini, saya ucapkan terima kasih.

#### Dosen

No	Pertanyaan	Ya	Tidak
1.	Apakah menurut anda fitur login dapat berfungsi dengan baik?		
2.	Apakah menurut anda fitur pemberitahuan dapat berfungsi dengan baik?		
3.	Apakah menurut anda fitur penggantian password dapat berfungsi dengan baik?		
4.	Apakah menurut anda fitur tugas akhir dapat berfungsi dengan baik?		
5.	Apakah anda dapat dengan mudah melihat data mahasiswa bimbingan tugas akhir?		
6.	Apakah menurut anda fitur mengunduh file tugas akhir dapat berfungsi dengan baik?		
7.	Apakah form catatan bimbingan dapat berfungsi dengan baik?		

#### Mahasiswa

No	Pertanyaan	Ya	Tidak
1.	Apakah menurut anda fitur pendaftaran user mudah untuk digunakan?		
2.	Apakah menurut anda fitur login mudah untuk digunakan?		

3.	Apakah menurut anda fitur penggantian password mudah digunakan?		
4.	Apakah menurut anda fitur pengiriman ide tugas akhir mudah digunakan?		
5.	Apakah anda dapat dengan mudah menerima notifikasi penerimaan ide tugas akhir?		
6.	Apakah anda dapat dengan mudah mengunggah file proposal atau tugas akhir anda?		
7.	Apakah fitur cetak form bimbingan mudah untuk digunakan?		
8.	Apakah menurut anda fitur login dapat berfungsi dengan baik?		
9.	Apakah menurut anda fitur penggantian password dapat berfungsi dengan baik?		
10.	Apakah menurut anda fitur pengiriman ide tugas akhir dapat berfungsi dengan baik?		
11.	Apakah anda dapat dengan mudah menerima notifikasi penerimaan ide tugas akhir?		
12.	Apakah menurut anda fitur mengunggah file tugas akhir dapat berfungsi dengan baik?		
13.	Apakah fitur cetak form bimbingan dapat berfungsi dengan baik?		

#### Admin

No	Pertanyaan	Ya	Tidak
1.	Apakah menurut anda fitur login dapat berfungsi dengan baik?		
2.	Apakah menurut anda formulir jurusan dan program studi dapat berfungsi dengan baik?		
3.	Apakah menurut anda menu mahasiswa dapat berfungsi dengan baik?		
4.	Apakah menurut anda menu dosen dapat berfungsi dengan baik?		
5.	Apakah menurut anda menu ubahan dapat berfungsi dengan baik?		
6.	Apakah menurut anda menu pengaturan dapat berfungsi dengan baik?		

Kritik dan Saran:

.....  
.....  
.....

Kota, Tanggal Bulan Tahun

(Nama Responden)